

CHIARIMENTI CIRCA IL CAPITOLATO PER LA LA FORNITURA DI UNA SOLUZIONE PER L'ADEGUAMENTO DEL SISTEMA INFORMATIVO DELL'ISTITUTO L. SPALLANZANI AL PROVVEDIMENTO DEL GARANTE DELLA PRIVACY DEL 27 NOVEMBRE 2008 E ALLE DISPOSIZIONI PRECEDENTI

1. Qual è il numero degli utenti registrati su Active Directory?

R: Il numero degli utenti registrati su Active Directory ammonta a circa 600

2. Quante persone sono impiegate nell'amministrazione dei sistemi?

R: Le persone impiegate nell'amministrazione dei sistemi sono 40, di cui 15 dipendenti dell'istituto e 25 dipendenti delle ditte fornitrici

3. Si richiede di conoscere la lista delle tipologie di server, sistemi operativi e rdbms interessati all'attività, ciascuna con le rispettive quantità.

R: Per quanto riguarda la lista dei server ,sistemi operativi e database interessati all' attività, ovvero che ospitano trattamenti relativi ai dati regolamentati dalla delibera del garante, si specifica quanto segue:

Server: Fujitsu Siemens Primergy n. 1 RX600, n. 6 RX300, n.1 Server Hp DL360, n.1 NAS HP X1600, n.2 Server Hp ML370, n.1 Server Hp 6000 PRO, n.1 server Dell PE 2009, un cluster formato da 2 Server Sun V480

Sistemi operativi: Windows Server 2000, 2003, 2008, Linux Redhat, Unix Solaris 5.9

RDBMS: MS SQLServer 2000, 2005, Sybase 10, Oracle 9.2, Ms Access, MSDE, Lotus Smartsuite, FileMaker 10, MySQL, PostGresql

4. Si richiede di indicare la tipologia e la quantità degli apparati da considerare nel perimetro.

R: Per quanto riguarda gli apparati da considerare nel perimetro dell'Istituto essi ammontano a circa 24 server (quelli coinvolti nell'attività sono elencati sopra), e circa 40 switch

5. Si richiede di fornire informazioni sulla componente mainframe da includere nel perimetro di attività.

R: Si specifica che non sono presenti Mainframe

6. Quanti server ospitano trattamenti relativi a dati regolamentati dalla delibera del garante?

R: Vedi punto 3

7. Quali sono i sistemi operativi che ospitano trattamenti relativi a dati regolamentati dalla delibera del garante?

R: Vedi punto 3

8. Quali sono i sistemi rdbms che ospitano trattamenti relativi a data regolamentati dalla delibera del garante?

R: Vedi punto 3

9. Si richiede di indicare la numerosità e ruolo del personale che deve essere sottoposto a cicli formativi

R: Il personale che deve essere sottoposto a cicli formativi è costituito da un Dirigente Analista e 4 Assistenti Tecnici Programmatori, tutti appartenenti alla U.O.S Informatica Integrata

10. *“... eventualmente da integrare con i già sistemi in essere (autenticazione di dominio, gruppi di utenti etc.)...”* Si richiedono dettagli su i sistemi da integrare
R: Per quanto riguarda i dettagli sui sistemi da integrare trattasi degli utenti , gruppi e policy registrati in MS Active Directory. Il sistema, tramite tale integrazione, deve consentire la gestione centralizzata dei profili di autenticazione/autorizzazione.
11. *“... per la gestione del sistema autenticazione/autorizzazione ed i profili di autorizzazione...”* per gestione si intende la predisposizione dell'identità ed il suo inserimento in gruppi
R: Per la gestione del sistema di autenticazione/identificazione si intende la predisposizione dell'identità, l'associazione del profilo all'utente e il suo inserimento in gruppi
12. Si richiede la fornitura dell'hardware necessario alla realizzazione della soluzione proposta?
R: La fornitura dell'Hardware necessario alla realizzazione della soluzione non è richiesta
13. Par. 9.2. Punto B: Si devono indicare i contenuti della documentazione che si intende rilasciare?
R: I contenuti della documentazione che dovrà essere fornita sono specificati nel capitolato speciale d'oneri e nell'allegato tecnico
14. Par. 9.2. Punto C: Esistono dei vincoli temporali per la realizzazione della soluzione?
R: La durata per la realizzazione della soluzione si ipotizza in un massimo di circa 3 mesi a partire dalla data di aggiudicazione
15. Per i log raccolti dal sistema di Log Management è richiesta la firma digitale? Oppure è sufficiente apporre il timestamp sui log ricevuti e renderli inalterabili e non modificabili?
R: Per i log raccolti dal sistema di Log Management è sufficiente l' apposizione del timestamp sui log che devono poi essere resi inalterabili e non modificabili
16. Quanti sono i server contenenti dati personali che si intende inserire nel sistema di log management?
R: Vedi punto 3
17. Per i server che andranno monitorati che tipo di sistema operativo è installato?
R: Vedi punto 3
18. Per la raccolta dei log la soluzione utilizzata deve essere esclusivamente agent-less? Nel caso c'è la necessità di installare un agent su ogni server questo crea problemi?
R: Per la raccolta dei log la soluzione sarà preferibilmente agent-less ma ciò non è un requisito vincolante
19. Il provvedimento del Garante richiede esclusivamente il tracciato dei login e logout effettuati dagli Amministratori sui server contenenti dati personali. Deve essere creata apposita reportistica con le informazioni aggiuntive richieste o è sufficiente che le informazioni aggiuntive siano comunque presenti e consultabili su una interfaccia web in modo da evitare che si abbiano report troppo pesanti e difficili da consultare?
R: Devono essere fornite le registrazioni degli accessi degli amministratori, comprendenti i riferimenti temporali e la descrizione dell'evento che le ha generate. Le registrazioni devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità. Altri report con i dati aggiuntivi\integrativi devono essere forniti separatamente ovvero consultabili online.

20. Relativamente alla richiesta della “lista degli Amministratori con i relativi permessi sui file di dati sensibili e le autorizzazioni di sistema” viene richiesto il log di suddette operazioni (cambio dei permessi su un file, autorizzazione di un nuovo utente ecc.), o la lista completa di ogni Amministratore con i relativi permessi e autorizzazioni?

R: Si intende che devono essere rese disponibili le informazioni atte a poter individuare “chi” ha effettuato l’accesso, “quando” l’accesso è stato fatto, “quale” file sensibile è stato coinvolto, “come” è stato eseguito l’accesso. Deve essere anche riportato il tipo di operazione eseguita: lettura, inserimento, modifica, cancellazione, backup, restore, etc. La lista completa di ogni Amministratore con relativi permessi ed autorizzazioni non è invece indispensabile

21. E’ possibile avere più dettagli del frame work applicativo per la gestione del sistema autenticazione/autorizzazione?

R: Vedi punto 10

22. Nel Vs. allegato B, alla lista dei documenti da allegare, si richiedono:

ELENCO DEI TRE PRINCIPALI SERVIZI RELATIVI AGLI ANNI 2007 2008 2009

Si fa presente che il provvedimento a cui si riferisce la Vs. richiesta di adeguamento è datata 27 novembre 2008 e quindi non ci sono i servizi effettuati antecedenti a questa data, ma solo nel 2009 e 2010.

R: Per “servizi principali” non si intende servizi “uguali” a quello in gara ma quelli ritenuti appunto principali dalla ditta partecipante e rappresentativi della propria competenza professionale.

23. Fase di collaudo e pre-esercizio: L'affidamento della fornitura si basa su un contratto di servizio che costituisce il riferimento sia per le attività del fornitore, sia per i controlli del committente. In tale a maggior chiarimento dell' Art. 19 del capitolato (“Verifica del servizio”) si specifica che la fase del collaudo sarà parte integrante della fornitura e assumerà valenza strategica principale per la verifica del servizio offerto. In tale fase, tramite un piano predisposto dal fornitore, si dovranno eseguire test da cui sia possibile verificare le funzionalità richieste del servizio, l'integrazione con gli ambienti, i sistemi e le altre applicazioni dell'istituto. Inoltre dovrà essere prevista la possibilità di registrare le eventuali non conformità ed anomalie rilevate, da rimuovere prima del rilascio della fornitura in esercizio. L' avvenuta esecuzione del collaudo sarà certificata da apposito verbale di collaudo controfirmata da entrambe le parti. Eseguito lo stesso si richiede la presenza della ditta aggiudicataria per 2 giorni di pre-esercizio, al fine di poter intervenire prontamente in caso si verificassero eventuali problematiche non evidenziate nella fase precedente.